



35. СРЕДНО ЕЗИКОВО УЧИЛИЩЕ „ДОБРИ ВОЙНИКОВ“

София 1164, район „Лозенец“, ул. „Добри Войников“ № 16, тел. 866 10 60, 963 37 31
e-mail: seu_35@35sou.bg, <https://35sou.bg>

**УТВЪРЖДАВАМ:
ВЕЛИЧКА ПЕТРОВА
ДИРЕКТОР НА 35 СЕУ**

ИНСТРУКЦИЯ

за мерките за защита на личните данни в 35.СЕУ „ДОБРИ ВОЙНИКОВ“

I. Общи положения

Чл. 1. (1) 35. СЕУ "Добри Войников" е юридическо лице със седалище град София, район Лозенец, ул. "Добри Войников" № 16, Република България с основен предмет на дейност образование и образователни услуги.

(2) Училището обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им, освен когато действа като обработващ лични данни за друг администратор или съвместно с друг администратор.

Чл. 2. Настоящата инструкция урежда организацията на обработването и защитата на лични данни на учителите, служителите, ученици, посетителите, както и на други физически лица, свързани с осъществяването на нормалната дейност на училището.

Чл. 3. (1) "Обработване" (на лични данни) означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(2) Обработването на лични данни се извършва само от лица, чиито служебни задължения или конкретно възложени задачи налагат извършването на обработка. Достъп до съхраняваните лични данни имат единствено лица, чиито служебни задължения или конкретно възложени задачи налагат такъв.

Чл. 4. Училището е Администратор (на лични данни) по смисъла на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

Чл. 5. (1) "Лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано ("субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) Принципите за защита на личните данни са:

1. Принцип на свеждане на данните до минимум - събирането на лични данни трябва да бъде в рамките на необходимото във връзка с целите, за които се обработват.
2. Принцип на законосъобразност, добросъвестност и прозрачност - информацията се събира и обработва по законен, прозрачен и обективен начин;
3. Принцип на ограничение на целите и на съхранението - личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона и в Общия регламент за защита на данните. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели и/или колкото е предвидено в нормативен акт. Личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1 от Общия регламент за защита на данните, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в Регламента с цел да бъдат гарантирани правата и свободите на субекта на данните (ако е приложимо);
4. Принцип на точност - личните данни трябва да са точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват;
5. Принцип на цялостност и поверителност - личните данни трябва да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

(3) В съответствие с чл. 35 от Общия регламент за защита на данните, оценката на въздействието се извършва при обработването на "чувствителни данни или данни от изключително лично естество" и "данни относно уязвими субекти на данни" (данни относно обучаемите ученици), в случаите на мащабно обработване на данни и на системно извършвано видеонаблюдение. Периодично, както и при промяна на характера на обработваните лични данни, броя на засегнатите физически лица и риска, с който са свързани операциите по обработване, се извършва преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни.

Чл. 6. Училището организира и предприема мерки за защита на личните данни от случайно или умишлено подправяне и/или унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) 35. СЕУ "Добри Войников" прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие. Многобройни критерии определят дали е необходимо

извършването на оценка на въздействието върху защитата на данните от 35. СЕУ "Добри Войников". Специфична оценка ще бъде извършвана винаги, когато дейността включва:

- ◆ регулярна и мащабна оценка на лични аспекти, свързани с физическите лица, която подлежи на автоматизирана обработка, включително профилиране, и на която се основават решения, които пораждаат правни последици или засягат по значителен начин физическото лице;
- ◆ обработка на голям обем специфични категории данни или на данни, свързани с присъди и нарушения; и/или
- ◆ широкомащабно наблюдение на публично достъпни зони.

При извършване на оценката и за осигуряване на съответствие се прилагат:

- Въпросник за оценка на въздействието върху защитата на данните (Приложение № 1),
- Въпросник за нивото на компетентност (Приложение № 1а),
- Процедура за оценка на въздействието върху защитата на данните (Приложение № 1б),
- Инструмент за оценка на въздействието върху защитата на данните (Приложение № 1в),
- Таблица за проверка на съответствието на договорите (Приложение № 1г),
- Наръчник за картографиране на движението на данни (Приложение № 1д),
- Процедура за разпределение на компетентността и отговорностите (Приложение № 1е),
- Опис на личните данни в организацията (Приложение № 1ж),
- Политика за водене и защита на записи (Приложение № 1з).
- Политика за информационна сигурност (Приложение № 1и).
- Декларация (политика) за поверителност на данните (Приложение № 1й).
- Уведомление - Декларация (политика) за поверителност на данните (Приложение № 1к).

(2) Съобразно резултатите от извършената оценка се установяват различни форми на защита:

1. Физическа защита;
2. Персонална защита;
3. Документална защита;
4. Защита на автоматизирани информационни системи и/или мрежи.

Чл. 8. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно, прозрачно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правни задължения на училището и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на училището се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразено с посочените мерки за защита и нивото на въздействие на съответния регистър.

Чл. 9. Личните данни могат да се обработват на следните основания:

1. за изпълнение на законово задължение от училището;
2. когато е наложително за защита на жизненоважните интереси на субекта на данните или на друго физическо лице;
3. когато е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на училището;
4. когато е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

5. когато е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

В случай че не е налице никое от изброените основания за обработка на личните данни, последната се извършва само след подписване на Декларация за съгласие от субекта на данни по образец (Приложение № 2).

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на училището.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции.

(4) Обработващите лични данни, част от персонала на Администратора, нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения. Обработващите лични данни, които имат достъп до лични данни, сключват с Администратора допълнително споразумение за поверителност по образец (Приложение № 3).

(5) Според случая и конкретните роли в правоотношението, с трети страни, Администраторът сключва споразумение за обработване на лични данни по образец (Приложение 3а) като прилага ОРЗД и Политиката за сключване на споразумение между администратора и обработващия лични данни и/или друг администратор (Приложение 3б).

Чл. 11. (1) Документите и преписките, по които работата е приключила, се архивират.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(3) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд и съгласно принципите, установени в Закона за защита на личните данни и Общия регламент за защита на данните.

(4) Документите на електронен носител се съхраняват на специализирани компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият лични данни и оторизираните длъжностни лица.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани лица.

Чл. 12. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, служителът, констатира това нарушение, докладва писмено за този инцидент на прекия си ръководител, който от своя страна е длъжен, своевременно да информира училищното ръководство.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

(3) Училищното ръководство/ОЗД следва незабавно (без ненужно забавяне) и не по-късно от 72 часа след като е разбрал за пробива в сигурността на данните да уведоми за нарушението на сигурността на личните данни Комисията за защита на личните данни. Уведомлението до Комисията се изготвя по образец (Приложение № 4) и съдържа причините за забавянето, когато не е подадено в срок от 72 часа и се прилага ОРЗД и Процедура за реагиране при инциденти по сигурността на информацията (Приложение № 4а)

(4) Училищното ръководство/ОЗД документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него, в нарочен регистър по образец (Приложение № 5) или образец (Приложение № 5а), в зависимост от конкретните технически възможности и ресурси на организацията.

Чл. 13. За всяко конкретно нарушение на сигурността на личните данни се съставя доклад по образец (Приложение № 6), който съдържа данни относно същността на нарушението на сигурността, засегнатите лични данни и степента, в която те са засегнати, последиците, настъпили от нарушението на сигурността, предприетите мерки и тяхната ефективност, както и заключение.

Чл. 14. При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, училището може да определи друго ниво на защита за регистъра.

Чл. 15. (1) След постигане целта на обработване, личните данни, съдържащи се във водените от училището регистри, следва да бъдат унищожени, освен ако не е въведено законово или секторно изискване или други, особено важни причини не налагат тяхното съхранение. При промени в структурата на училището, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(2) Когато основанието за обработка е съгласие на субекта на данни, в случай на възражение срещу обработката или на оттегляне на съгласието на субекта, обработката следва да бъде преустановена и данните да бъдат заличени. Личните данни се изтриват и при постъпило искане от субекта, в случай че са налице посочените в чл. 17 от Общия регламент за защита на данните условия.

(3) В случаите, когато се налага унищожаване на носител на лични данни, училището прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и

злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(4) Унищожаване се осъществява от служителя, отговорен за архива на училището.

Чл. 16. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление (Приложение № 7), респ. искане за упражняване на права на субектите на данни, след тяхното идентифициране. Постъпилите искания от субектите на данни се завеждат в нарочен регистър (Приложение № 8) или образец (Приложение № 8а), в зависимост от конкретните технически възможности и ресурси на организацията, като се следва Процедура при направено искане на субект на данни (Приложение № 8б).

(2) Решението си за уважаване или отхвърляне на искането на съответното лице, училището съобщава без ненужно забавяне (препоръчително в 30-дневен срок от подаване на заявлението, респ. искането).

(3) Срокът по ал. 2 може да бъде удължен от администратора с 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора или е необходимо отправяне на запитване за становище от надзорния орган.

(4) Информацията може да бъде предоставена под формата на:

1. (по изключение чрез) устна справка;
2. (приоритетно чрез) писмена справка;
3. преглед на данните от самото лице, в случай че не се наруши неприкосновеността на други лица;
4. предоставяне на исканата информация на технически и/или електронен носител.

(5) Изключение се допуска единствено за тези органи и/или институции, които извършват това въз основа на изискване на закона (напр. МОН, МВР, съд, прокуратура, НАП, НОИ и др.).

II. Мерки по осигуряване на защита на личните данни

Чл. 17. (1) Физическа защита в училището се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(2) Основните приложими организационни мерки за физическа защита в училището включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп. Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна

само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения.

(3) Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(4) Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим за изпълнение на служебните им задължения. Като зони с контролиран достъп се определят всички помещения на територията на училището, в които се събират, обработват и съхраняват лични данни. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(5) Основните приложими технически мерки за физическа защита в училището включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Чл. 18. (1) Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на политиката и ръководствата за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. забрана за споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
5. съгласие за поемане на задължение за неразпространение на личните данни.

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа "Необходимост да знае".

(4) Лицата могат да започнат да обработват лични данни след запознаване с:

1. нормативната уредба в областта на защитата на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора;
4. нивото на достъп до информация, съответстващо на тяхната длъжностна характеристика.

Чл. 19. (1). Основните приложими мерки за документална защита на личните данни са:

1. Определяне на регистрите, които съдържат лични данни, и се поддържат на хартиен носител: на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на училището;

2. Определяне на условията за обработване на лични данни: личните данни се събират и обработват само по реда и при условията на ЗЗЛД, ОРЗД, настоящата инструкция и други релевантни документи, издадени от училищното ръководство;
3. Регламентиране на достъпа до регистрите: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на "Необходимост да знае";
4. Определяне на срокове за съхранение: личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.
5. Процедури за унищожаване: Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, след изтичане на законовите срокове за тяхното съхранение, в случай че не са необходими за нормалното функциониране на училището, се унищожават по подходящ и сигурен начин (напр. нарязване, електронно изтриване и други подходящи за целта методи).

Чл. 20. (1) Защитата на автоматизираните информационни системи и/или мрежи в училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

1. Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на училището. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа "Необходимост да знае";
2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото въвеждане, поддръжка и обработка;
3. Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от системния администратор.
4. Политиката по създаване и поддържане на резервни копия за възстановяване - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.
5. Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)
6. Персоналната защита на данните е част от цялостната охрана на училището.
7. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.
8. Данните, които вече не са необходими за целите на училището и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване или постоянно заличаване от електронните средства).

III. Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка

Чл. 21. (1) Електронен (компютърен) достъп до файлове, съдържащи лични данни, се осъществява само от обработващи лични данни с регламентирани права, единствено от тяхното

физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.

(2) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на отпадане на основанието за достъп до лични данни, правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 22. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 23. (1) В училището се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице - системен администратор.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и Общия регламент за защита на данните и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 24. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП) по смисъла на Закона за електронния документ и електронните удостоверителни услуги, нямат право да предоставят издания им КЕП на трети лица.

IV. Поддържани регистри и тяхното управление

Чл. 25. Поддържаните от 35.СЕУ "Добри Войников" регистри с лични данни са:

1. Относно Ученици
 - 1.1. Регистър - Електронни дневници;
 - 1.2. Регистър - НЕИСПУО
 - 1.3. Регистър - Сведение за организацията и дейността в учебното заведение за учебната година;
 - 1.4. Регистър - Библиотечни картони;
 - 1.5. Регистър - Архив.
2. Относно Персонал
 - 2.1. Регистър - Персонал.
3. Относно Родители
 - 3.1. Регистър - Родители
4. Относно Контрагенти
 - 4.1. Регистър - Контрагенти.
5. Относно Посетители
 - 5.1. Регистър - Пропускателен режим.
6. Относно Видеонаблюдение
 - 6.1. Регистър - Видеонаблюдение.

Чл. 26. (1) В регистрите относно "Ученици" се събират и съхраняват лични данни с цел индивидуализиране и обучение на физическите лица "ученици", обучавани в училището.

(2) Общо описание на регистрите относно "Ученици"

Регистрите съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;
2. културна идентичност: интереси и хоби;
3. социална идентичност - образование;
4. семейна идентичност - родствени връзки;
5. лични данни, които се отнасят до здравето.

Нормативното основание е Законът за предучилищното и училищно образование /ЗПУО/, ЗЗО, КСО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистрите относно "Ученици":

♦ носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на обработващите лични данни, снабдени със защитна сигнализация. Информацията от хартиените носители за всеки ученик, се записва в регистрите, както следва:

1.1. Регистър - НЕИСПУО.

Регистърът се води от упълномощено лице със заповед на директора.

Данните от регистъра се предоставят доброволно от лицата при записването им.

Право на достъп до данните в регистъра имат:

- Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

- Директорът, заместник-директори, главният счетоводител, учителите и секретарят при изпълнение на правомощията им по Кодекса на труда и на обичайните им задължения съгласно длъжностна характеристика.

- Държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в който се посочва основаниято, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

1.2. Регистър - Електронни дневници е предназначен за вписване на информация за резултатите от учебната дейност на всеки ученик в една паралелка за една учебна година и съдържа имена и оценки.

Регистърът се води от класния ръководител и всеки учител, който преподава в класа, и се контролира от заместник-директора по учебната дейност.

Данните в регистъра се събират за лицата в процес на обучението им в учебното заведение.

Право на достъп до данните в регистъра имат:

- Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;

- Директорът, ЗДУД, главният счетоводител, ръководител на направление ИКТ, учителите и ЗАС при изпълнение на правомощията им по Кодекса на труда и на обичайните им задължения съгласно длъжностна характеристика.

- Държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в който се посочва основаниято, имената на лицата, на които е необходимо да се осигури достъп до личните данни. Данните от регистъра могат да бъдат предавани по електронен път.

Регистърът се води от класния ръководител и се контролира от Директора.

1.3. Регистър - Сведение за организацията и дейността в учебното заведение за учебната година (Списък-образец № 1) е предназначен да служи за установяване на съответствието на

организацията на учебния процес с нормативната уредба в системата на предучилищното и училищното образование. Той обслужва информационно нуждите на МОН, РУО, НОИ, общинската или районната администрация и финансиращите органи. Списък-образец №1, съдържа реквизитите, посочени в приложение № 1 към Наредба 8/2016 г. за информацията и документите за системата на предучилищното и училищно образование.

Към Списък - образец № 1 се прилагат: документи за статута на училището в случаите, в които е настъпила промяна през предшестващия период; прилаганите в училището учебни планове; утвърдените учебни програми за преподаваните предмети от раздели Б и В на учебния план в общообразователните училища и раздели В и Г в професионалните училища; годишен план на училището; дневен режим на институцията.

Право на достъп до данните в регистъра имат:

- Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, ЗДУД, главният счетоводител, ръководител направление ИКТ, учителите и секретарят - при изпълнение на правомощията им по Кодекса на труда и на обичайните им задължения съгласно длъжностна характеристика.
- Държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в който се посочва основаниято, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

Данните от регистъра могат да бъдат предавани по електронен път.

1.4. Регистър - Библиотечни картони е предназначен за вписване на информация при ползване на материали от библиотечния фонд на училището в читални и заемни и съдържа имена, ЕГН и данни за контакт с учениците с цел идентифициране на лицата и защита от недобросъвестно поведение с библиотечния фонд.

Библиотечните картони се съхраняват при отговорника за библиотечния фонд на училището.

Право на достъп до данните в регистъра имат:

- Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, ЗДУД, главният счетоводител, учителите и секретар при изпълнение на правомощията им по Кодекса на труда и на обичайните им задължения съгласно длъжностна характеристика.

Данните от регистъра не могат да бъдат предавани по електронен път и служат за изготвяне на съответните удостоверения за преместване, удостоверения за завършен клас и свидетелства за завършен клас, които остават у приносителя.

Регистърът се води от отговорника за библиотечния фонд и се контролира от Директора.

1.5. Регистър - Архив;

В регистър Архив се съхраняват лични данни:

♦ На работилите в учебното заведение по трудови правоотношения, на физическите лица, сключили договори със заведението на различни основания, както и на други лица, предоставили доброволно личните си данни;

♦ На учащите се и учителите в учебното заведение;

1. Съхраняване на предоставените документи в предвидените срокове;

2. Изпълнение на нормативните изисквания на Кодекса на труда, ЗПУО, Наредба 8/2016г. за информацията и документите за системата на предучилищното и училищно образование, Закона за задълженията и договорите, Закона за Националния архивен фонд, Номенклатурата за водене и съхранение на делата, Инструкция за документооборота и др.;

3. Използване на събраните данни за служебни цели, свързани с изготвяне на справки, издаване на документи и други статистически и исторически цели, при спазване на принципите и процедурите, описани в настоящата инструкция.

Формата на водене на регистъра е на хартиен носител:

1. Данните се съхраняват в писмена (документална) форма и се класират в архивни дела, съответстващи на въведената инструкция за архивиране /деловодна обработка/
2. Делата се подреждат в специални шкафове, които са разположени в изолирано помещение със защитна сигнализация.
3. Обработващите лични данни предприемат всички организационни мерки за съхраняването и опазването на делата, в това число изолиране на достъпа до тях на външни лица и служители.
4. Делата не се изнасят извън сградата на администратора.

В регистър Архив се съхраняват следните категории лични данни:

1. Относно физическата идентичност на лицата: имена, ЕГН, адрес по местоживееене и др.;
2. Относно семейната идентичност на лицата: семейно положение - наличие на брак, развод, брой на децата в семейството и тяхната възраст и др.;
3. Относно образованието: степен на образованието, придобита специалност, допълнителна квалификация и др.;
4. Относно трудовата дейност: професионална биография, трудов стаж и др.;
5. Относно здравния статус на лицата;
6. Относно гражданско-правния статус на лицата: свидетелство за съдимост;
7. Относно икономическата идентичност: финансово състояние и др.;

Срок на съхранение: съгласно Номенклатурата на делата в 35.СЕУ "Добри Войников" със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистрите относно "Ученици" са: ЗДУД, ЗДАСД, ЗАС и класни ръководители, както и целият педагогически персонал.

Обработващите лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Нивото на въздействие на регистрите относно "Ученици" по отношение на различните критерии е, както следва:

1. Поверителност - ниско ниво;
2. Цялостност - ниско ниво;
3. Наличност - ниско ниво;
4. Общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи).

Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители са защитени по адекватен начин, в зони с контрол на достъпа.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, както и чрез поддържане на информацията и на хартиен носител.

(7) 35. СЕУ "Добри Войников" предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от 35. СЕУ "Добри Войников" - предприемат се конкретни действия в зависимост от конкретната ситуация;
 2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
 3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.
- Във всички случаи на повреда на регистри/документи, съдържащи лични данни, които може да доведат до риск за субекта на данни, незабавно се уведомява Комисията за защита на личните данни и потенциално засегнатия субект.

(8) Достъп до регистрите относно "Ученици" имат и държавните органи - МОН, РУО, дирекция "Социално подпомагане" за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните и съхранявани лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни на учениците се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в 35. СЕУ "Добри Войников".

(10) След постигане целите по предходната алинея личните данни на учениците се унищожават физически, чрез нарязване, за което се изготвят актови протоколи за унищожаване.

Чл. 27. (1) Относно родители на ученици се води регистър "Родители", в който се събират и съхраняват лични данни с цел индивидуализиране на физически лица - родители, настойници и други категории, свързани с учениците лица.

(2) Общо описание на регистър "Родители". Регистърът съдържа следните категории данни:

1. физическата идентичност - име, адрес, телефони за връзка и месторабота;
2. икономическа идентичност - финансово състояние;
3. социална идентичност - образование, трудова дейност;
4. семейна идентичност - семейно положение и родствени връзки.

Нормативното основание е ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър "Родители":

◆ носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на Обработващите лични данни, снабдени със защитна сигнализация. - На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно Номенклатурата на делата в 35. СЕУ "Добри Войников" със срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни в регистър "Родители" са: ЗДУД, гл. счетоводител, ЗДАСД, секретар и класни ръководители, както и целият педагогически персонал.

Обработващите лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическият достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до електронните системи, обработващи лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители са защитени по адекватен начин в зони с контрол на достъпа.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства. Защитата на електронните данни от неправомерен достъп (пароли) се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

(7) 35. СЕУ "Добри Войников" предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от 35 СЕУ "Добри Войников" - предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

Във всички случаи на повреда на регистри/документи, съдържащи лични данни, които може да доведат до риск за субекта на данни, незабавно се уведомява Комисията за защита на личните данни и потенциално засегнатия субект.

(8) Достъп до регистър "Родители" имат и държавните органи - МОН, РУО, дирекция "Социално подпомагане" за изпълнение на техните задължения, предвидени в съответните закони и подзаконовни нормативни актове.

Достъп до обработваните и съхраняваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в 35. СЕУ "Добри Войников".

(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез нарязване, за което се изготвят актови протоколи за унищожаване.

Чл. 28. (1) Относно персонала на Администратора се води регистър "Персонал", в който се събират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или по граждански договори.

(2) Общо описание на регистър "Персонал" Регистърът съдържа следните категории данни:

1. физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;
2. психологическа идентичност - документи относно психическото здраве;
3. социална идентичност - образование и трудова дейност;
4. семейна идентичност - семейно положение и родствени връзки;
5. лични данни, които се отнасят до здравето;
6. други - лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

Предназначението на събираните данни в регистъра е свързано с :

1. Индивидуализиране на трудовите правоотношения;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.;
4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(3) Технологично описание на регистър "Персонал":

♦ носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудова досиета). Папките се подреждат в шкафови, които са разположени в изолирани заключващи се помещения на Обработващите лични данни, снабдени със защитна сигнализация.
- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма "Ком Си": счетоводство, финансов контролор. Базата данни се намира на твърдия диск на изолирани компютри.
- Срок на съхранение: съгласно Номенклатурата на делата в със 35. СЕУ "Добри Войников" срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър "Персонал" са: ЗДАСД и гл. счетоводител.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до електронните системи, обработващи лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители са защитени по адекватен начин в зони с контрол на достъпа.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Трудовите досиета на персонала не се изнасят извън сградата на училището.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на училището.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и Общия регламент за защита на данните и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(7) 35. СЕУ "Добри Войников" предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от 35. СЕУ "Добри Войников" - предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

Във всички случаи на повреда на регистри/документи, съдържащи лични данни, които може да доведат до риск за субекта на данни, незабавно се уведомява Комисията за защита на личните данни и потенциално засегнатия субект.

(8) Достъп до регистър "Персонал" имат и държавните органи - НАП, НОИ, МОН, РУО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните и съхраняваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изисквали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в 35. СЕУ "Добри Войников".

(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез нарязване, за което се изготвят актови протоколи за унищожаване.

Чл. 29. (1) Относно "Контрагенти" се води регистър "Контрагенти", в който се събират и съхраняват лични данни с цел индивидуализиране на физически и/или физически лица, представители на юридически лица, доставящи/предоставящи/даряващи съответно продукти и/или услуги на 35. СЕУ "Добри Войников".

(2) Общо описание на регистър "Контрагенти" Регистърът съдържа следните категории данни:

1. физическата идентичност - име, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка и банкови сметки;
2. други - лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

Предназначението на събираните данни в регистъра е свързано с:

1. Индивидуализиране на правоотношенията;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключване, съществуване, изменение и прекратяване на правоотношения, изготвяне на договори, допълнителни споразумения, заповеди и др.;
4. Установяване на връзка със служители и други лица по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията им.

(3) Технологично описание на регистър "Контрагенти":

♦ носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения на Обработващите лични данни, снабдени със защитна сигнализация.

- На технически носител: Личните данни се въвеждат в специализирана счетоводна програма "Ком Си": счетоводство, финансов контролор. Базата данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно Номенклатурата на делата в със 35. СЕУ "Добри Войников" срокове на съхранение;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър "Контрагенти" са: ЗДАСД и гл. счетоводител.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. Достъпът до електронните системи, обработващи лични данни, е ограничен чрез уникални

потребителски идентификатори и пароли, а електронните носители са защитени по адекватен начин в зони с контрол на достъпа.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Трудовите досиета на персонала не се изнасят извън сградата на училището.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на училището.

При внедряване на нов програмен продукт за обработване на лични данни се проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и Общия регламент за защита на данните и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(7) 35. СЕУ "Добри Войников" предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от 35. СЕУ "Добри Войников" - предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

Във всички случаи на повреда на регистри/документи, съдържащи лични данни, които може да доведат до риск за субекта на данни, незабавно се уведомява Комисията за защита на личните данни и потенциално засегнатия субект.

(8) Достъп до регистър "Контрагенти" имат и държавните органи - НАП, НОИ, МОН, РУО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните и съхраняваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в 35. СЕУ "Д. Войников".

(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез нарязване, за което се изготвят актови протоколи за унищожаване.

Чл. 30. (1) Относно посетители се води регистър "Пропускателен режим", в който се събират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.

(2) Общо описание на регистър "Пропускателен режим"

Регистърът съдържа следните категории данни - физическата идентичност: име по лична карта и адрес.

(3) Технологично описание на регистър "Пропускателен режим": Данните се въвеждат в писмена форма в дневник.

(4) Определяне на длъжностите:

Обработващи лични данни на регистър "Пропускателен режим" са служителите ангажирани с охраната и ЗДАСД.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическият достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(7) Действия за защита при аварии, произшествия и бедствия: обработващият лични данни изнася дневника при евакуация.

(8) Достъп до регистър "Пропускателен режим": Категориите лица, на които личните данни могат да бъдат разкривани, са физическите лица, за които се отнасят данните, и други лица, ако е предвидено в нормативен акт.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват (до приключване на дневника).

(10) След приключване на дневника, воден на хартиен носител, същият се унищожава физически, чрез изгаряне.

(11) Източниците, от които се събират данните, са физическите лица - субекти на данните.

(12) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на училището.

Чл. 31. (1) Относно видеонаблюдението на територията на училището се води регистър "Видеонаблюдение", в който се събират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Общо описание на регистър "Видеонаблюдение":

Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградата на училището.

Регистърът съдържа следните категории данни - физическата идентичност на лицето - видеообраз.

(3) Технологично описание на регистър "Видеонаблюдение": Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и

посетителите на територията на училището, както и при провеждане на ДЗИ, НВО - VII и X клас и провеждане на изпити на ученици в самостоятелна форма на обучение.

(4) Определяне на длъжностите:

Обработващи лични данни на регистър "Видеонаблюдение" са служителите ангажирани с охраната.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическият достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(7) Категориите лица, на които личните данни могат да бъдат разкривани, са физическите лица, за които се отнасят данните, и други оторизирани лица, ако е предвидено в нормативен акт.

(8) Лични данни се съхраняват в паметта на дивииара за срок от 14 дни. При необходимост записите могат да бъдат свалени на външен носител съгласно закона и след оформяне на протокол в писмена форма.

(9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.

(10) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на училището.

Чл. 32. (1) В "Регистър на администратора на лични данни" се описват дейностите по обработване, които осъществява администраторът, по образец (Приложение № 9) или образец (Приложение № 9а), в зависимост от конкретните технически възможности и ресурси на организацията.

(2) Определяне на задълженията:

Отговорен за съставяне и поддържане на "Регистър на администратора на лични данни" е директорът.

(3) Организационни мерки за физическа защита:

Регистърът се поддържа в електронна форма. Достъп до него има единствено администраторът на лични данни. Приложими за всички описани в настоящата инструкция технически и организационни мерки за защита на устройството, на което се съхранява регистърът.

(4) Категориите лица, на които личните данни могат да бъдат разкривани, са длъжностни лица от Комисията за защита на личните данни в предвидените в закона и в ОРЗД случаи.

(5) Данните в регистъра се обновяват, когато е наложително, при промяна в дейността на администратора.

Чл. 33. (1) В "Регистър на обработващия лични данни" се описват дейностите по обработване, които осъществява всеки обработващ лични данни, по образец (Приложение № 10) или образец (Приложение № 10а), в зависимост от конкретните технически възможности и ресурси на организацията.

(2) Определяне на длъжностите:

Отговорен за съставяне и поддържане на "Регистър на обработващия лични данни" е всяко лице, което обработва лични данни от името на администратора.

(3) Организационни мерки за физическа защита:

Регистърът се поддържа в електронна форма. Достъп до него има администраторът на лични данни и лицето, което го съставя и поддържа (обработващият лични данни). Приложими за всички описани в настоящата инструкция технически и организационни мерки за защита на устройството, на което се съхранява регистърът.

(4) Категориите лица, на които личните данни могат да бъдат разкривани, са длъжностни лица от Комисията за защита на личните данни в предвидените в закона и в ОРЗД случаи.

(5) Данните в регистъра се обновяват, когато е наложително, при промяна в дейността на администратора и/или на обработващия лични данни.

V. Права и задължения на отговорника по защита на данните и на лицата, обработващи лични данни

Чл. 34. (1) Отговорник по защита на личните данни (ОЗД) се назначава от Директора на училището, като ОЗД може да съвместява и други длъжности.

(2) ОЗД трябва да познава Регламент (ЕС) 2016/679, Закона за защита на личните данни, другите разпоредби за защита на данните в българското законодателство, политиката за поверителност на данните и вътрешните правила и процедури, както и да следи практиката на надзорния орган.

(3) ОЗД следи за съответствието на ежедневната работа с политиката за защита на данните, Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ЗЗЛД и свързаното законодателство, като и има следните задължения: Да осигурява прилагането на политиката за защита на данните; Да разработва и постоянната поддържа и подобряване политиката за защита на данните; Непрекъснато да подобрява квалификацията и преквалификацията си и да повишава компетентността си в областта на политиката за защита на данните; Да осигурява и поддържа система за информираност и обучение на служителите по отношение на изискванията за съответствие с Регламента, наложени от приетите правила и процедури; Да преглежда и одобрява процедурите

и правилата, съгласно които се обработват лични данни (например: създаването, управлението и промяната на уведомленията за поверително третиране на личните данни; обработка на искания от субектите на данни, включително искания за достъп, поправка, изтриване и др.; събирането и обработването на лични данни; работа по жалби във връзка с обработването на лични данни; управлението на случаите на нарушения на данните, свързани със сигурността; и управление на взаимодействието с трети страни по въпросите свързани със защитата на лични данни); Да поддържа връзка с лицата, отговорни за оценка на въздействието и въпросите на сигурността; Да предоставя експертни съвети и насоки по въпроси, свързани със законодателната и регулаторната защита на данните; Да извършва тълкуването и прилагането на различните изключения, приложими към обработването на лични данни; Да съветва и да информира за оценката риска и необходимостта от оценка на въздействието върху защитата на данните и да следи изпълнението на изискванията на ОРЗД; Да предоставя съвети във връзка с проекти, свързани със споделяне на данни (включително въпроси, свързани със сигурността, когато данните са извън работното място); Да следи всички изменения на законодателството и съответните разяснения, свързани със законодателството за защита на данните и своевременно да информира ръководството на администратора; Да извършва редовни проверки относно съответствие на правилата за защита на данните и промените в законодателството, практиката и технологиите; Да извършва създаването, подаване и управление на уведомления до надзорния орган, когато това се изисква съгласно Регламента и други разпоредби за защита на данните; Да прилага, когато е удачно, практиките, свързани с обработването на лични данни, посочени в съществуващите задължителните или препоръчителни кодекси за поведение.

(4) Дава становища и препоръки относно Регламент (ЕС) 2016/679, Закона за защита на личните данни, другите разпоредби за защита на данните в българското законодателство, политиката за поверителност на данните и вътрешните правила и процедури, както и да следи практиката на надзорния орган.

Чл. 35. Служителите на училището са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица, за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 36. (1) За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Допълнителни разпоредби

§ 1. По смисъла на настоящата инструкция:

- ◆ "Лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано ("субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.
- ◆ "Специални категории лични данни" означава лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни, отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.
- ◆ "Администратор" е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.
- ◆ "Администратор" (на лични данни) е 35. СЕУ "Добри Войников" (училището).
- ◆ "Ниво на защита" е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.
- ◆ "Обработване" (на лични данни) е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.
- ◆ "Обработващ лични данни" е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.
- ◆ "Оценка на въздействие" е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.
- ◆ "Поверителност" е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
- ◆ "Предоставяне на лични данни" са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.
- ◆ "Регистър с лични данни" означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.
- ◆ "Съгласие на физическото лице" е всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени.
- ◆ "Права на субектите на данни" означава:
 - Право на информираност съобразно Съображения 58, 60-62 от Преамбюла и член 12-14 от Общия регламент относно защитата на данните;

- Право на достъп съобразно Съображение 63 от Преамбюла и член 12 и 15 от Общия регламент относно защитата на данните;
- Право на прехвърляне на личните данни на друг администратор (право на преносимост на данните) съобразно Съображение 68 от Преамбюла и член 12 и 20 от Общия регламент относно защитата на данните;
- Право на коригиране съобразно член 5, 12, 16 и 19 от Общия регламент относно защитата на данните;
- Право на изтриване ("правото да бъдете забравени") съобразно Съображения 65 и 66 от Преамбюла и член 6, 9, 12 и 17 от Общия регламент относно защитата на данните;
- Право на ограничаване на обработването съобразно Съображение 67 от Преамбюла и член 18 и 19 от Общия регламент относно защитата на данните;
- Право на възражение срещу обработването съобразно Съображения 69 и 70 от Преамбюла и член 12 и 21 от Общия регламент относно защитата на данните.
- Право на жалба срещу обработването, като компетентният за това орган е Комисия за защита на личните данни с адрес: гр. София 1592, бул. ""Проф. Цветан Лазаров" № 2 Интернет страница: www.cpdp.bg ; Електронна поща: kzld@cpdp.bg; Център за информация и контакти - тел. 02/91-53-518
- ♦ "Получател" означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за "получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;
- ♦ "Трето лице" е физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

Преходни и заключителни разпоредби

§ 2. Всички служители на училището са длъжни срещу подпис да се запознаят с инструкцията и да я спазват.

§ 3. Настоящата инструкция се издава на основание чл. 23, ал. 4 от Закона за защита на личните данни и Общия регламент за защита на данните.

§ 4. За всички неуредени в настоящата инструкция въпроси са приложими разпоредбите на Закона за защита на личните данни, Общия регламент за защита на данните и действащото приложимо законодателство на Р България.

§ 5. Всички Приложения (регистри, процедури, бланки, въпросници и др.) към настоящата инструкция, независимо дали са инкорпорирани в основния текст или са допълнително посочени като Приложения, са неразделна част от правилата и ги детайлизират, където е необходимо.

§ 6. Инструкцията е утвърдена със Заповед № ЛС-226 от 07.12.2020 година.

ПРИЛОЖЕНИЕ № 1

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИ ДАННИ

ВЪПРОСНИК

Този формуляр се използва за запис на ключова информация относно оценка на въздействието върху защитата на личните данни, която може да бъде изисквана съгласно Общия регламент за защита на данните (ОРЗД).

Информация за дейността

Наименование на дейността:	
Референтен номер на дейността:	
Описание на дейността:	

Основание на оценката на въздействието върху защитата на лични данни

Моля, изберете причината, поради която оценката на въздействието върху защитата на лични данни е подходяща:

- ☐ Информацията за лицата ще бъде събирана и обработвана за първи път
- ☐ Информацията за лицата ще бъде споделена с хора или организации, които преди не са имали достъп до нея
- ☐ Променя се използването на съществуващите лични данни
- ☐ Използва се нова технология, която да събира или използва данни от личен характер (биометрични)
- ☐ Съществуващите лични данни ще бъдат използвани за вземането на решения като част от автоматизиран процес
- ☐ С основание може да бъде очаквано, че човек може да намери аспект от дейността като вмешателство или да намери включените данни за поверителни
- ☐ Друга причина (моля, конкретизирайте):

Обхват на оценката на въздействието върху защитата на лични данни

Определете обхвата според географското разположение, спецификите на дейността, засегнатите субекти, организационните единици и ИТ системите

Включени лични данни

Опишете елементите на данните, които ще бъдат събирани и обработвани.

Как ще бъдат получени данните?

Опишете дали данните ще бъдат получени директно от субекта на данните или индиректно от трето лице.

Как ще бъдат обработени данните?

За какво ще бъдат използвани данните? Ще бъдат ли предавани на една или повече трети страни?

Какви са сроковете за съхранение на данните? Защо?

Как ще бъдат съхранявани данните?

Къде ще бъдат съхранявани данните и какъв контрол ще бъде установен?

Има ли друга възможна употреба на данните?

Има ли вероятност данните да бъдат използвани за цели, различни от тези, за които се събират, и ако да - за какви?

Къде ще бъдат изпратени данните и при какви условия?

Ще бъдат ли изпратени данните в страни извън Европейския съюз? Ако да, до какво ще доведе изпращането, има ли необходимите гаранции и защо то е наложително?

Кой ще има достъп до данните и как?

Кой от организацията и кои външни лица ще имат достъп до данните и какъв контрол ще има, за да се управлява достъпът?

Подпис:	
Име:	
Дата:	

ДОКЛАД

ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИ ДАННИ

1. Въведение

Целта на този доклад е да представи констатациите от задачата за оценяването на защитата на лични данни от до с обхвата, описан по-долу. Главната цел на задачата е да оцени рисковете за правата и свободите на субектите на данни, с оглед на събраните и обработени лични данни от 35.СЕУ "Д. Войников" и да определи кои от тях могат да бъдат приети и кои имат нужда от предприемане на мерки за справяне с тях.

След като докладът е одобрен, изпълнението на определени действия, които са описани в него, ще бъде ръководено до приключване като част от проекта. Процесът, използван за това оценяване, е изложен в документа "Процедура за оценка на въздействието върху защитата на личните данни".

Този доклад описва:

- ▶ предложените операции за обработване и информацията за включените лични данни;
- ▶ целите на обработването, включително, където е приложимо, законния интерес на 35. СЕУ "Д. Войников", както е определено в Общия регламент за защита на личните данни (ОРЗД);
- ▶ оценка на необходимостта и пропорционалността на обработването;
- ▶ резултатите от оценяването на рисковете за правата и свободите на субектите на данни;
- ▶ дали всеки риск се препоръчва за приемане или третиране;

- ▶ приоритет на рисковете за третиране;
- ▶ отговорници за рисковете;
- ▶ препоръчани опции за третиране;
- ▶ мерки за контрол, които да бъдат приложени;
- ▶ отговорност за набелязаните действия;
- ▶ срокове за действия
- ▶ остатъчни стойности на риска, след като са приложени мерки.

Докладът трябва да бъде подписан от висшето ръководство преди да си продължи по-нататък.

Оценяването беше проведено от следните лица:

Таблица 1 - Екип Рисково оценяване

Име	Роля в оценяването
	Водещ рисков оценител
	Асистент рисков оценител

Като част от оценяването, следните лица бяха консултирани:

Таблица 2 - Консултирани лица

Име	Длъжност	Местоположение
-----	----------	----------------

2. Контекст на оценяването

Тази секция описва причините, поради което е било проведено оценяването, активите на личните данни, които са били в неговия обхват и критериите, които са били приложени, за да се реши кои рискове се препоръчват за приемането.

2.1. Вътрешен и външен контекст

(Описание на вътрешния и външния контекст на оценяването, както е определено в документа "Процедура на оценяването на взаимодействието върху защитата на лични данни". Това трябва да включва причините, поради които е проведено оценяването и възможните ползи от него.)

--

2.2. Обхват

(Граници на оценяването по отношение на проблемите и елементите, които покрива или не покрива.)

--

2.3. Предложени операции по обработване

(Описание на механизма на предложеното обработване, включително как ще изглежда, как личните данни ще бъдат събирани, използвани, съхранявани и премахвани)

--

Личните данни, които ще бъдат събирани и използвани като част от обработването са следните:

Вид лични данни	Описание	Предложено обработване
Име	(Три) имена на субекта на данни	Използване заедно с Дата на раждане, за да се идентифицира лицето
Дата на раждане	Точна дата на раждане във формат дд.мм.гггг	Използвана заедно с Име, за да се идентифицира лицето и да се определи възрастова граница за участие на учениците в някои дейности.
Адрес	Пълният адрес на клиента, включително пощенски код	Използвано за писмена кореспонденция
Пол	Полът, с който лицето се идентифицира	Използва се за идентифициране на подходящите за ученика дейности

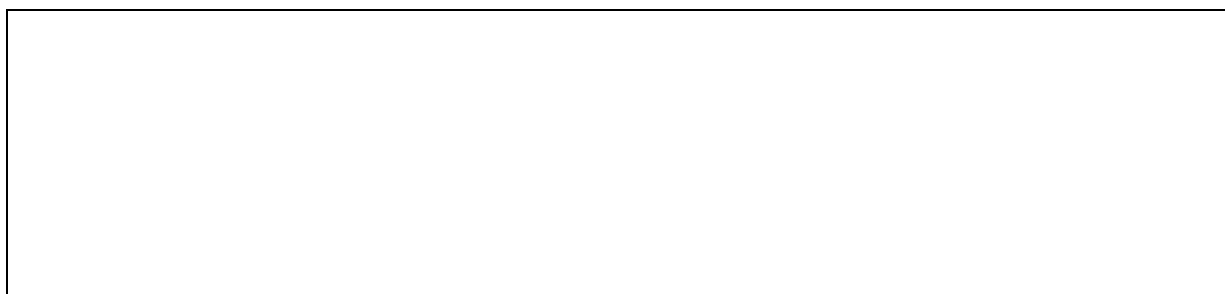
2.4. Цели на обработването

(Описание на целта на обработването на лични данни и какви ползи може да има за субекта на данни и за училището, включително, където е приложимо, легитимният интерес на училището по смисъла на Общия регламент за защита на данните).



2.5. Необходимост и пропорционалност на обработването

(Описание на причините, поради които е необходимо събирането на посочените категории лични данни, и защо е невъзможно дейността да се извърши без личните данни да бъдат предоставени. Когато е приложимо се посочват техниките за псевдонимизация и усилията, положени за свеждане на данните до минимум в процеса на обработване.)



2.6. Критерии за приемане на риска

С оглед достигане до заключение за това кои рискове са на достатъчно високо ниво, за да се нуждаят от по-нататъшно третиране, са използвани определен брой критерии, за да се оцени нивото на приемливостта. Един риск се препоръчва за приемане, ако:

- Рискът е преценен като нисък или среден
- Оценката показва, че рискът е възможно да съществува в рамките на три или по-малко месеца
- Очаква се потенциалните преки или косвени ползи да бъдат по-големи от негативното въздействие.

Причините, поради които се препоръчва приемането, са описани по-долу:

--

Обобщение на резултатите от оценяването на риска

Обобщение на резултата от оценката на риска е показано в Таблица 3 по-долу.

Обосновка и изводи от осъществената оценка на риска

Реф. номер	Кратко обобщение на риска	Описани е на риска	Отговорник по риска	Ниво на риска	Приеман е или третиране	Приоритет на третиране	Коментари
1.							
2.							
3.							
4.							
5.							
6.							
7.							

План за третиране на риска

№	Описание на риска	Отговорник по риска	Ниво на риска	Вид третиране	Действие	Отговорник	Период	Остатъчно ниво на риска
1.								
2.								
3.								
4.								
5.								
6.								

ПРИЛОЖЕНИЕ № 1А - ВЪПРОСНИК ЗА НИВОТО НА КОМПЕТЕНТНОСТ (.XLS)

ПРИЛОЖЕНИЕ № 1Б - ПРОЦЕДУРА ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ (.DOC)

ПРИЛОЖЕНИЕ № 1В - ИНСТРУМЕНТ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО (.XLS)

ПРИЛОЖЕНИЕ № 1Г - ТАБЛИЦА ЗА ПРОВЕРКА НА СЪОТВЕТСТВИЕТО НА ДОГОВОРИТЕ (.DOC)

ПРИЛОЖЕНИЕ № 1Д - НАРЪЧНИК ЗА КАРТОГРАФИРАНЕ НА ДВИЖЕНИЕТО НА ДАННИ (.XLS)

ПРИЛОЖЕНИЕ № 1Е - ПРОЦЕДУРА ЗА РАЗПРЕДЕЛЕНИЕ НА КОМПЕТЕНТНОСТТА И ОТГОВОРНОСТИТЕ (.DOC)

ПРИЛОЖЕНИЕ № 1Ж - ОПИС НА ЛИЧНИТЕ ДАННИ В ОРГАНИЗАЦИЯТА (.XLS)

ПРИЛОЖЕНИЕ № 1З - ПОЛИТИКА ЗА ВОДЕНЕ И ЗАЩИТА НА ЗАПИСИ (.DOC)

ПРИЛОЖЕНИЕ № 1И - ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ (.DOC)

ПРИЛОЖЕНИЕ № 1Й - ДЕКЛАРАЦИЯ (ПОЛИТИКА) ЗА ПОВЕРИТЕЛНОСТ (.DOC)

ПРИЛОЖЕНИЕ № 1К - УВЕДОМЛЕНИЕ - ДЕКЛАРАЦИЯ (ПОЛИТИКА) ЗА ПОВЕРИТЕЛНОСТ (.DOC)

ПРИЛОЖЕНИЕ № 2

ФОРМУЛЯР ЗА ИСКАНЕ НА СЪГЛАСИЕ ЗА ОБРАБОТКА НА ДАННИ

Този формуляр може да се използва за предоставяне на изрично съгласие за обработка на лични данни, съгласно разпоредбите на Общия регламент за защита на данните (ОРЗД). Той трябва да се използва заедно с подходяща декларация за поверителност.

Кои сме ние?

Настоящият формуляр Ви се предоставя от 35. СЕУ "Д. Войников". Съгласието, което предоставите чрез настоящия формуляр, ще бъде използвано само и единствено от училището, като Вашите данни няма да бъдат предоставяни на трети страни.

Бихме искали да използваме следната информация за Вас:

1. ►
2. ►
3. ►
4. ►

Защо бихме искали да използваме предоставената информация?

--

Какво ще правим с Вашата информация?

--

Как да оттеглите съгласието си?

--

--

Моля, предоставете ни следната информация:

Ако сте съгласни да предоставите исканата информация, моля, посочете я по-долу.

1. ►	
2. ►	
3. ►	
4. ►	

Моля, попълнете този раздел, за да покажете съгласието си

Име:	
Дата:	
Подпис:	

Попълненият формуляр може да се изпрати на електронна поща,
да бъде предоставен на хартиен носител на място в училището или да бъде изпратен на
хартиен носител по пощата на адрес

ПРИЛОЖЕНИЕ № 3

СПОРАЗУМЕНИЕ ЗА ПОВЕРИТЕЛНОСТ НА СЛУЖИТЕЛЯ

Като част от своята дейност, 35. СЕУ "Д. Войников" може да изисква от своите служители да достъпват и обработват поверителна информация от името на училището (вътрешна информация) или от името на друга организация. В такива случаи е важно основанието, въз основа на което поверителната информация (вкл. лични данни) е споделяна, да се документира и тълкува. Също така участващите трети страни трябва да

гарантират, че тази информация ще бъде защитена по подходящ начин във всеки един момент. Настоящият документ е образец на споразумение за поверителност, което може да бъде използвано директно или като отправна точка за създаване на споразумение, съобразено с конкретните обстоятелства.

1. 35. СЕУ "Д. Войников" възнамерява да разкрие*, наричана по-нататък "поверителната информация" на служителя за целта на** , наричана по-нататък "целта".

2. Служителят се съгласява да не използва поверителната информация за друга цел, освен описаната по-горе, без преди това да вземе изричното писмено съгласие на 35. СЕУ "Д. Войников".

3. Служителят се задължава да опазва поверителната информация и да пречи за нейното разкриване на която и да е трета страна, освен ако последната не е обвързана със задължения, равностойни на тези в клауза 2.

4. Описаните по-горе клаузи 2 и 3 се отнасят до цялата поверителна информация, предоставена от 35. СЕУ "Д. Войников" на служителя, независимо от метода или формата. Клаузите не се отнасят за:

а) всяка информация, която към датата на споразумението или по-късно излезе в публичното пространство (освен ако преди това информацията е била предмет на настоящето споразумение); или

б) всяка информация, която вече е била известна на служителя към датата на настоящето споразумение и която не е обхваната от отделно споразумение за поверителност.

5. Нищо в това споразумение няма да преклудира правото на служителя да разкрие поверителната информация, когато това се изисква съгласно закон или от компетентен орган.

6. Служителят се задължава, въз основа на писмено искане на 35. СЕУ "Д. Войников", да върне всички записи на поверителната информация на 35. СЕУ "Д. Войников" и да гарантира, че копия на тази информация не са запазени от него или от трети страни, на които поверителната информация е била разкрита.

7. Това споразумение не предоставя на служителя патент или участие по отношение на правата върху интелектуалната собственост на 35. СЕУ "Д. Войников", с изключение на правото да прави допустими копия на поверителната информация, ако това е необходимо за описаната в споразумението цел.

8. Гаранциите, описани в клаузи 2 и 3, ще продължат да са в сила за*** от датата на това споразумение.

9. За това споразумение се прилага българският закон и правото на Европейския съюз.

Българските държавни съдилища ще имат юрисдикцията да решават спорове, които може да възникнат от или във връзка с това споразумение.

Име на служителя	Длъжност	Дата	Подпис

* Опишете информацията, която ще бъде разкрита, вкл. личните данни, които училището обработва

** Опишете целите на разкриването, напр. осигуряване на административна поддръжка за обработването.

*** Уточнете броя на годините/месеците или въведете фиксиран краен срок.

Приложение № 3а

СПОРАЗУМЕНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Днес [-] .20.. г. в гр. София между

1. [-], наричан за краткост [-] или

- ☐ АДМИНИСТРАТОР
- ☐ ОБРАБОТВАЩ ЛИЧНИ ДАННИ
- ☐ (ПОД)ОБРАБОТВАЩ ЛИЧНИ ДАННИ

(Отбелязва се само една роля, като в случай на застъпване на роли се сключва отделно писмено споразумение)

от една страна и

2. [-], наричан/а/о за краткост [-] или

- ☐ АДМИНИСТРАТОР
- ☐ ОБРАБОТВАЩ ЛИЧНИ ДАННИ
- ☐ (ПОД)ОБРАБОТВАЩ ЛИЧНИ ДАННИ

(Отбелязва се само една роля, като в случай на застъпване на роли се сключва отделно писмено споразумение)

от друга страна,

(наричани заедно „Страните“, а всеки от тях поотделно „Страна“)

ПРЕДВИД ЧЕ:

А) Страните по настоящото Споразумение са страни по Договор № [-] от [-] за [-]/договорите описани в Приложение № 1 – неразделна част от Споразумението;

Б) Страните по настоящото Споразумение и по договора (ите) от б. „А“ по-горе и желаят да уредят отношенията си по *Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните (ОРЗД), Закона за защита на личните данни (ЗЗЛД) и свързаното законодателство;*

на основание:

☐ чл. 26 от ОРЗД (Съвместни администратори)

☐ чл. 28 от ОРЗД (Администратор/Обработващ лични данни/и друг обработващ)

се сключи настоящото Споразумение, както следва:

Дефиниции

„Администратор“ на лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на ЕС или в правото на държава членка.

„Обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора

„Обработване на лични данни“ е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване

„Съвместни администратори“ означава когато двама или повече администратори съвместно определят целите и средствата на обработването

„Съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени

„Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

1. *(Неприложимото се зачертава)* АДМИНИСТРАТОРИТЕ/АДМИНИСТРАТОРЪТ/ ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ и *(Неприложимото се зачертава)* ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ / (ПОД) ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ се съгласяват да обработват конкретно посочените в настоящото Споразумение лични данни и други данни, при условията на Споразумението. В случаите по чл. 26 от ОРЗД АДМИНИСТРАТОРИТЕ могат, при необходимост, допълнително да детайлизират съответните роли и връзки между тях и спрямо субектите на данни в Приложение № 2 - неразделна част от Споразумението, като съществените характеристики на договореността трябва да са достъпни за субекта на данните.

2. Страните приемат да обработва посочените лични данни и други данни в съответствие с условията на настоящото Споразумение и съгласно ОРЗД, ЗЗЛД и свързаното законодателство.

3. Страните се съгласяват личните данни и други данни да се обработват от *(неприложимото се зачертава)* АДМИНИСТРАТОРИТЕ/ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ/(ПОД) ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ и техните служители при условия на конфиденциалност, *(неприложимото се зачертава)* със собствени и/или наети ресурси и за нуждите на изпълнението на настоящото Споразумение, при необходимата организация за обработването и за защитата на личните и други данни от нерегламентиран достъп, в съответствие с писмените указания на АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ или в случаите по чл. 26 от ОРЗД съгласно уговореното писмено между АДМИНИСТРАТОРИТЕ.

4. *(Неприложимото се зачертава)* АДМИНИСТРАТОРИТЕ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД) ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ получава (т) достъп до: (i) следните категории лични данни *(напр. име, национален идентификационен номер, номер на документ за самоличност, националност, етническа принадлежност, дата на раждане, телефон, имейл, адрес, позиция, работодател, пол, здравен статус, риск от заболявания, хранителни предпочитания, кръвна група, фотографски материали, номер на полет, дестинация, място на отсядане, период на отсядане и др. - да се посочи приложимото)*:

..... и (ii) следните категории други данни (напр. за организации, технически данни и др. - да се посочи приложимото):

Горепосочените данни се отнасят само до следните категории лица (напр. пълнолетни лица от мъжки/женски пол и др. - да се посочи приложимото):

..... и ще се обработват само със следните средства (напр. писмено и в електронна форма, само чрез посочените видове електронни носители и др. - да се посочи приложимото):

..... и за следните цели (напр. информационен бюлетин (вкл. на трети страни), маркетинг и реклама (вкл. от трети страни), автоматизирано вземане на решения (включително профилиране), и др. - да се посочи приложимото):

5. (Неприложимото се зачертава) АДМИНИСТРАТОРИТЕ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД) ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ има (т) право да обработва (т) личните данни и другите данни посочени в чл. 4 по-горе, изключително и само във връзка със сключеното Споразумение, само за посочените цели и с посочените средства, като предприема (т) действия съгласно писмените указания на АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ или в случаите по чл. 26 от ОРЗД съгласно уговореното писмено между АДМИНИСТРАТОРИТЕ.

6. (Неприложимото се зачертава) АДМИНИСТРАТОРЪТ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД) ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ декларира (т) и гарантира (т), а (неприложимото се зачертава) другият АДМИНИСТРАТОР/ ОБРАОТВАЩИЯТ ЛИЧНИ ДАННИ се съгласява (т), че личните данни и другите данни посочени в чл.4 по-горе ще бъдат обработвани и съхранявани отделно от всякакви други бази данни:

- ☐ на територията на Европейския съюз;
- ☐ на територията на трети държави;
- ☐ в облачни структури.

7. (Неприложимото се зачертава) АДМИНИСТРАТОРЪТ/ ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ може да осъществява контрол над процеса на обработване на данните, като в рамките на редовното работно време на (неприложимото се зачертава) другия АДМИНИСТРАТОР/(ПОД)ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ може да извършва проверки, без да нарушава работния процес.

8. (Неприложимото се зачертава) АДМИНИСТРАТОРЪТ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ се съгласява, че (неприложимото се зачертава) другият АДМИНИСТРАТОР/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД)ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ може да ангажира ОБРАБОТВАЩ ЛИЧНИ ДАННИ/ (ПОД)ОБРАБОТВАЩ ЛИЧНИ ДАННИ, при необходимост и по своя преценка с писменото съгласие на (неприложимото се зачертава) другия АДМИНИСТРАТОР /АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ като ангажиралият ги носи отговорност за техните действия като за свои пред

(неприложимото се зачертава) другия АДМИНИСТРАТОР /АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ.

9. *(Неприложимото се зачертава)* АДМИНИСТРАТОРЪТ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ надлежно запознава ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ/(ПОД)ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ/другия АДМИНИСТРАТОР с правилата, политиките и процедурите, които е приел и ги прилага за защита на личните данни и за другите данни. В случай, че се установи необходимост от извършване на Оценка на въздействието на защитата на данните (ОВЗД) по чл. 35 от ОРЗД и/или друг вид оценка на баланса спрямо правата на субектите на данни, Страните си оказват необходимото съдействие по закон.

10. *(Неприложимото се зачертава)* ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД)ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/АДМИНИСТРАТОРИТЕ води (ят) задължителните регистри по чл. 30 от ОРЗД и предотвратява (т) всякакъв незаконен или случаен достъп до личните данни или други данни, промяната на същите, унищожаването или загубата им, незаконно прехвърляне и всякакво друго незаконно обработване, както и всеки друг вид злоупотреба с тях. За целите на изпълнение на това свое задължение Страните прилагат необходимата техническа и организационна защита по глава IV, Раздел 2 от ОРЗД, включително се уведомяват незабавно за установени нарушения на сигурността, с необходимите подробности и си оказват необходимото съдействие при уведомяване на надзорния орган и съобщаване на субектите на данни. В случаите, когато е задължително по закон, Страните определят и длъжностно лице по защита на данните (ДЛЗД) по чл. 37 от ОРЗД. Промени в предмета на настоящото Споразумение и методите на обработка на данните са допустими само чрез сключването на допълнително писмено споразумение между страните.

11. *(Неприложимото се зачертава)* ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД)ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/АДМИНИСТРАТОРА незабавно информира *(неприложимото се зачертава)* другия АДМИНИСТРАТОР /АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ, ако счита че някое от получените от него указания са в противоречие с разпоредбите на ОРЗД, ЗЗЛД или друго приложимо законодателство. Съответното указание може да не бъде изпълнено, докато не бъде изрично писмено потвърдено. Лицата, които имат право да дават указания от страна на [-] са:..... (име, позиция, отдел, телефон, имейл).

Лицата, упълномощени да приемат указания от страна на [-] са:.....

(име, позиция, отдел, телефон, имейл).

Лицата, упълномощени да приемат указания от страна на [-] са:.....

(име, позиция, отдел, телефон, имейл).

В случаите по чл. 26 от ОРЗД АДМИНИСТРАТОРИТЕ определят точка за контакт за субектите на данни за целите на настоящото Споразумение, както следва:

.....

(име, позиция, отдел, телефон, имейл).

12. *(Неприложимото се зачертава)* АДМИНИСТРАТОРЪТ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ има право да прекрати настоящото Споразумение без предизвестие при:

- грубо нарушение от страна на *(неприложимото се зачертава)* другия АДМИНИСТРАТОР /АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ/ (ПОД)ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ на условията на Споразумението или

- при отказ на задължената страна да изпълни писмени указания на другата Страна, освен ако е налице хипотеза по чл.12 и предполагаемо противоречие на такова указание със закона или

- възпрепятстване на *(неприложимото се зачертава)* другия АДМИНИСТРАТОР /АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ от задължената страна при осъществяването на контрол по чл. 7.

13. При всяко прекратяване, освен ако друго не е уговорено в настоящото Споразумение или писмено указано от *(неприложимото се зачертава)* АДМИНИСТРАТОРА, ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ *(неприложимото се зачертава)* ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ/(ПОД)ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ се задължава да унищожи всички съхранявани от него лични данни и други свързани записи и данни, ако не бъде указано друго, в срок не по-късно от 30 дни от датата на прекратяване на Споразумението, като преди това писмено предложи да предаде копие от данните в подходящ вид на *(неприложимото се зачертава)* АДМИНИСТРАТОРА/ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ. В случаите по чл. 26 от ОРЗД АДМИНИСТРАТОРИТЕ се споразумяват писмено как да действат в посочения 30-дневен срок от датата на прекратяване на Споразумението.

14. *(Неприложимото се зачертава)* АДМИНИСТРАТОРИТЕ/ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ и АДМИНИСТРАТОРА/ ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ и (ПОД)ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ носят отговорност пред субектите на лични данни за обработването извършено по настоящото Споразумение по реда предвиден в глава VIII от ОРЗД и по ЗЗЛД, като всяко нарушение подлежи на конкретно установяване и ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ се освобождава от отговорност, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

14.1. АДМИНИСТРАТОРЪТ, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава ОРЗД, а ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ носи отговорност за вреди, произтичащи от извършеното обработване, само когато не е изпълнил задълженията по ОРЗД, конкретно насочени към ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ, или когато е действал извън законосъобразните указания на АДМИНИСТРАТОРА или в противоречие с тях.

14.2. Когато в една и съща операция по обработване участват повече от един АДМИНИСТРАТОР или ОБРАБОТВАЩ ЛИЧНИ ДАННИ или участват и АДМИНИСТРАТОР, и ОБРАБОТВАЩ ЛИЧНИ ДАННИ, всеки администратор или обработващ лични данни носи отговорност за цялата вреда, за да се гарантира действително обезщетение на субекта на данни.

14.3. Когато АДМИНИСТРАТОР или ОБРАБОТВАЩ ЛИЧНИ ДАННИ е изплатил пълното обезщетение за причинената вреда, той има право да поиска от другите АДМИНИСТРАТОРИ или ОБРАБОТВАЩИ ЛИЧНИ ДАННИ, участвали в същата операция по обработване на лични данни, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда в съответствие с ОРЗД.

14.4. Страните се съгласяват и потвърждават, че ще си съдействат в рамките на закона при изпълнението на изискванията по ОРЗД, глава III от ОРЗД, включително при (i) обработването на постъпили искания, (ii) предоставяне на информация, (iii) изпълнение на указания на надзорния орган, (iv) извършване на одити и други.

15. Страните по настоящото Споразумение се съгласяват и потвърждават, че са запознати с политиките, процедурите и правилата на другата (ите) Страна (и) и ще ги зачитат при изпълнението на ангажиментите си по настоящото Споразумение.

16. За неуредените в настоящото Споразумение въпроси се прилагат разпоредбите на ОРЗД, КЗЛД и свързаното българско и европейско законодателство.

17. Настоящото Споразумение влиза в сила на [-].20.. г. и е валидно до [-].20.. г.

Настоящото Споразумение се състави в два екземпляра – по един за всяка от Страните.

За [-]:

За [-]:

Приложение № 3Б - ПОЛИТИКА ЗА СКЛЮЧВАНЕ НА СПОРАЗУМЕНИЕ МЕЖДУ АДМИНИСТРАТОРА И ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ И/ИЛИ ДРУГ АДМИНИСТРАТОР (.DOC)

Приложение № 4

УВЕДОМЛЕНИЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Този формуляр е предназначен да се използва от служител (отговорник по защита на данните) на 35. СЕУ "Д. Войников", за да уведоми Комисията за защита на личните данни за

нарушението на сигурността на личните данни в съответствие с изискванията на Общия регламент за защита на данните.

Детайли на уведомлението

Име на лицето, подавало уведомлението:	
Длъжност:	
Име на организацията:	
Адрес на организацията:	
Телефонен номер:	
Електронна поща:	
Дата и час на подаване на уведомлението:	
Дата и час на установяване на нарушението на сигурността на личните данни:	
Изминало време между установяването на нарушението и уведомяването:	

Описание на естеството на нарушението на сигурността на личните данни
--

--

Евентуални последици от нарушението на сигурността на личните данни
--

--

Предложени мерки, които да се предприемат за справяне с нарушението

--

Предприети мерки за справяне с нарушението

--

Причини за забавяне на уведомлението, ако е приложимо

[illegible]

ПРИЛОЖЕНИЕ № 4А - ПРОЦЕДУРА ЗА РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА (.DOC)

Приложение № 5

Регистър на нарушения на сигурността на личните данни

[illegible]

ПРИЛОЖЕНИЕ № 5А - РЕГИСТЪР НА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ (.XLS)

Приложение № 6

35. СЕУ "Д. Войников"
град София, район Лозенец, ул. "Д. Войников" № 16, Република България
тел. 02/ 866 10 60, 02/ 963 37 31, e-mail sou_35@abv.bg

град София, район Лозенец, ул. "Д. Войников" № 16, Република България

тел. 02/ 866 10 60, 02/ 963 37 31, e-mail sou_35@abv.bg

ДОКЛАД ЗА НАРУШАВАНЕ СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

ДАННИ ЗА КОНТАКТ		
Име	Организация	За контакт
	Длъжност: 35. СЕУ "Д. Войников"	тел.: ел. поща:

ОБОБЩЕНА ИНФОРМАЦИЯ
<i>(Резюме на събитието и обстоятелствата - кога, какво, кой, обобщение на инцидента)</i>

ЗАСЕГНАТИ ЛИЧНИ ДАННИ			
ТИП	ЧУВСТВИТЕЛНОСТ	ОБХВАТ	ВЕРОЯТНИ ПОСЛЕДСТВИЯ
<i>Име</i> <i>Дата на раждане</i> <i>Данни за здравословно състояние</i> <i>Друго</i>	<i>(ниска/висока)</i>	<i>Всички ученици</i> <i>Служители</i> <i>Родители</i>	

ПРЕДПРИЕТИ ИЛИ ПРЕДЛОЖЕНИ МЕРКИ	
МЕРКИ	ДАТА

ЗАКЛЮЧЕНИЕ

Сериозно/незначително нарушение, вероятност да се случи отново, ефективност на предприетите мерки

Приложение № 7

ИСКАНЕ ОТ СУБЕКТА НА ЛИЧНИ ДАННИ

Този формуляр следва да послужи за предоставяне на искане от субекта на лични данни съгласно Общия регламент за защита на данните (ОРЗД).

Детайли за подателя:	
Длъжност (ако е приложимо):	
Име:	
Адрес:	
Идентификатор на субекта:	

Тип на искането:

Моля, посочете типа на искането, което правите:

- ☐ Оттегляне на съгласие
- ☐ Искане за достъп
- ☐ Коригиране на личните данни
- ☐ Изтриване на лични данни
- ☐ Ограничение за обработване на лични данни
- ☐ Искане за преносимост на лични данни
- ☐ Възражение за обработване на лични данни
- ☐ Искане относно автоматизирано вземане на решение и профилиране.

Лични данни, за които се отнася искането:
--

--

Детайли на искането:

--

Основание на искането/обосновка:

--

Подпис:	
Име:	
Дата:	

Попълненият формуляр следва да се изпрати по електронна поща на адрес,
да се предостави на място в училището или да се изпрати на хартиен носител по пощата на
адрес

Приложение № 8

Регистър на исканията от субекта на лични данни

Исканията от субектите на лични данни да упражняват правата си съгласно
GDPR трябва да бъдат регистрирани тук

**Последна
актуализация:**

Актуализиран от:

Дата на искането	Титла/ Обръщение	Име/идентифи- кационен номер	Адрес	Вид на искането	Включени лични да
---------------------	---------------------	------------------------------------	-------	--------------------	-------------------

ПРИЛОЖЕНИЕ № 8А - РЕГИСТЪР НА ИСКАНИЯТА ОТ СУБЕКТА НА ЛИЧНИ ДАННИ (.XLS)

ПРИЛОЖЕНИЕ № 8Б - ПРОЦЕДУРА ПРИ НАПРАВЕНО ИСКАНЕ ОТ СУБЕКТА НА ЛИЧНИ ДАННИ (.XLS)

Приложение № 9 - Регистър на администратора на лични данни

**ПРИЛОЖЕНИЕ № 9А - РЕГИСТЪР НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ
(.DOC)**

Приложение № 10 - Регистър на обработващия лични данни

Обработващ лични данни			
Име и данни за връзка		Отговорник по защита на данните	
Име		Име	
Адрес		Адрес	
Email		Email	
Телефон		Телефон	

Име и данни за връзка на администратора	Същност (категории) на обработката	Категории субекти на данни	Категории лични данни	График за изтриване на категориите лични данни (ако е възможно)	О

ПРИЛОЖЕНИЕ № 10А - РЕГИСТЪР НА ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ (.DOC)